



Action Property Management

CCTV Privacy Impact Assessment (PIA)

1. Introduction and Purpose of CCTV Systems

1.1 This CCTV Privacy Impact Assessment (PIA) is recommended in The Surveillance Camera Code of Practice, issued by the Surveillance Camera Commissioner in June 2013, Amended November 2021, in accordance with Section 30 (1) (a) of The Protection of Freedom Act 2012. The purpose of the PIA is to ensure that privacy risks are minimised where CCTV is used by Action Property Management.

1.2 Guidance is based on the ICO's Privacy Impact Assessment Handbook accessed on 16th December 2024.

The four areas which are highlighted by ICO as potential areas for loss of privacy in relation to personal data are;

- The privacy of personal information;
- The privacy of the person;
- The privacy of personal behaviour;
- The privacy of personal communications

1.3 Personal data' as defined by Section 1 of the Data Protection Act means data which relates to a living individual who can be identified:

- From data.
- From data and other information (such as door entry information where recorded) which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

1.4 When considering the installation of a camera an Operational Requirement (OR) must be produced. The OR must be referred to as part of the installation and camera review process to ensure it meets and continues to be effective in addressing the purpose for which it was installed.

1.5 The CCTV systems that we manage are intended to provide an increased level of security for the residential buildings where CCTV systems are located.

1.6 The CCTV systems are used to respond to the following legitimate aims / key objectives, which will be subject to annual assessment.

- To detect, prevent or reduce the incidence of crime including theft and burglary.
- To determine the liability of any damage caused to the development.
- To prevent and respond effectively to all forms of noise disturbances, harassment and public disorder.
- To reduce the fear of crime.
- To create a safer community.
- To gather evidence by a fair and accountable method.
- To provide emergency services assistance.
- To assist with health and safety including monitoring flood levels at Emperors Wharf.
- To monitor and enforce the use of car parking bays.

2. Responsible Person Contact Details

Below are the contact details of the person most qualified to respond to questions regarding this Privacy Impact Assessment.

Name: Matthew Ward

Title: Managing Director

Organisation: Action Property Management

Email: m.ward@actionpropertymanagement.co.uk

Telephone: 0113 2442210

A.	Why is a privacy impact assessment required	
1.1	<p>What is the aim of the surveillance system?</p>	<p>In line with Action Property Managements CCTV Code of Practice, use of the CCTV's system located at the residential sites we manage shall be for the purpose of:-</p> <ul style="list-style-type: none"> • To detect, prevent or reduce the incidence of crime including theft and burglary. • To determine the liability of any damage caused to the development. • To prevent and respond effectively to all forms of noise disturbances, harassment and public disorder. • To reduce the fear of crime. • To create a safer community. • To gather evidence by a fair and accountable method. • To provide emergency services assistance. • To assist with health and safety including monitoring flood levels at Emperors Wharf. • To monitor and enforce the use of car parking bays.
1.2	<p>What organisations will have access to CCTV images?</p> <p>Who will take legal responsibility under the Data Protection Act?</p>	<p>Action Property Personnel are the only users of the CCTV system, Police Forces and law enforcement agencies will be granted access to the system if a legitimate request is received.</p> <p>Action Property Management is the Data Controller at the point of images being recorded, however if any images are released to any of the authorised organisations, then the legal responsibility will be transferred to that organisation in relation to the images that have been released.</p>
1.3	<p>What are the benefits to be gained from the system and who will benefit?</p>	<p>CCTV is a proven tool in assisting with block property management and detecting / deterring crimes, and the perpetrators of it. Using CCTV can significantly reduce the time and cost in investigating issues / allegations.</p>
1.4	<p>Can CCTV realistically deliver these benefits?</p>	<p>Yes</p>

B	Information Flow	
2.1	How is information collected?	The systems provides video footage which is recorded on a DVR in secure areas of each of the sites we manage.
2.2	Where are the real time images from the camera displayed?	Images are displayed on a monitor in a secure area at each of the sites we manage. The footage is not monitored and is only used in the event of an incident occurring.
2.3	Who has operational access to the CCTV camera?	Each site we manage has either (1) Property Manager (2) Caretaker (3) Concierge who have access to the CCTV. No access is provided to the management company / leaseholders or residents.
2.4	How are the images recorded?	Camera footage is continuously recorded by way of a Digital Video Recorder.
2.5	Where are the recorded images stored?	On the Hard Drives of Digital Video Recorders, which are housed within a secure area at each residential site. Should a request be made by law enforcement agencies then footage may be retained on a memory stick (safe) until we are advised we can dispose
2.6	How is information stored?	A digital recording and data management system is in place which covers all data collected by all CCTV recordings.
2.7	What measures are in place to control access to the area in which the recorded images are stored?	Access to areas where CCTV is kept is restricted to the Property Manager / Caretaker / Concierge.
2.8	How is information used	CCTV is used to enhance the management of the residential sites that we manage the the reasons declared in Section 1.
2.9	How is access gained to the recorded images?	Data management control levels are established on the systems with password controls on all systems.
2.10	How long are the images retained?	21 days, unless requested as part of an incident and then stored on archive until investigations are complete.
2.11	How is information deleted	The data management system automatically deletes information after 21 days or before if the hard drives become full.
2.12	When data is downloaded or copied for release to a third party how is information recorded?	Via USB memory stick.
2.13	What processes are in place to ensure that data protection responsibilities are understood by persons receiving the data?	Each request for data must be agreed by the Responsible Person who will ensure that appropriate measures are in place to ensure data protection responsibilities are met. Unless a request is made for personal data under GDRP then data is only provided to authorised public agencies such as law enforcement / fire and rescue services / coroner and the court service.

2.14	What precautions are in place to ensure that data will continue to be collected e.g. in the event of a failure of power to cameras and DVR (?)	None. The cost of providing back up power is outweighed by the benefit of recording loss.
C	Data Protection	
3.1	Can less privacy intrusive solutions achieve the same objectives?	<p>CCTV is the best possible solution.</p> <p>To mitigate the system impact, public areas are masked to avoid intrusion. Occasionally viewing of these areas is required on a temporary basis (for example to monitor flood water levels on the highway adjacent at Emperors Wharf in York).</p> <p>We do inform members of the public that CCTV is in use by installing signs detailing the scheme and its purpose, along with a contact telephone number.</p>
3.2	Are images of identifiable individuals required or could the scheme use other technology not cable of identifying individuals?	<p>The system must be capable of identifying individuals, as footage from the system may be used in both criminal and civil court cases.</p> <p>If our systems did not have this capability, it would not be fit for purpose.</p>
3.3	Will the particular equipment / system of work being considered deliver the desired benefits now and remain suitable in the future?	Yes
3.4	What future demands may arise for wider use of images and how will you address these?	Legislation can and does change. We will comply with all future regulations placed upon us.
3.5	What are the views of those under surveillance?	By abiding with current legislation, we aim to show that the CCTV system is only used for management of the residential development and for crime reduction / detection purposes.
D	Human Rights	
4.1	What could we do to minimise intrusion for those that may be monitored, particularly if specific concerns have been expressed? Is the system established on a proper legal basis and operated in accordance with the law?	<p>The system has been established on a proper and legal basis and we comply with the Data Protection Act, Human Rights Act and Regulations of Investigatory Powers Act.</p> <p>Employees using the system are provided with adequate training.</p> <p>Regular reviews of camera locations are undertaken to justify their need.</p>
4.2	Is CCTV justified in the circumstances?	Yes
4.3	Is it proportionate to the problem that it is designed to deal with?	Yes. CCTV is used for only the purposes stated and complies with the current legislation.

E	Surveillance code of practice	
5.1	Do you regularly review the system against its objectives?	Yes, an annual review is undertaken or when legislation changes
5.2	Is the system being used for any other purpose other than those specified?	No
5.3	Does signage exist highlighting the use of surveillance cameras?	Yes
5.4	Does the signage highlight the point of contact?	Yes
5.5	Are all staff aware of their responsibilities?	Yes
5.6	Can a member of the public request footage?	Yes. The procedure of Data Subject Access requests is located on the APM Website. CCTV footage can only be supplied for up to 21 days from the date and time of an incident, after which time the images are automatically overwritten.
F	Risks	
6.1	Is the data shared with other organisations	Yes, for investigation and enforcement
6.2	Is the system operated in full compliance with: <ul style="list-style-type: none"> • DPA • Requirements of the ICO Code Practice • SCC Code Practice • Human Rights Act 	Yes
6.3	Do you have procedures in place to manage risks associated with the use of the CCTV system	Yes
G	Privacy Solutions	
7.1	Have you identified solutions to address any risks identified	The system is operated in line with relevant legislation and codes of practice.

Author: Matthew Ward

Document created: 16/12/24

Document reviewed: 29/01/25